Policy #: DHHS-01-13

I. SUBJECT

Health Information Privacy and Security Executive Policy

The Department shall comply with applicable health information privacy and security requirements, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules, as updated by the Health Information Technology for Economic and Clinical Health Act (HITECH), and other applicable federal and state laws, regulations and rules relating to the confidentiality of identifiable consumer information.

II. POLICY STATEMENT

It is the policy of the Department of Health and Human Services (the Department) to fully comply with the requirements of HIPAA, HITECH, as well as federal and state laws, regulations, rules, accreditation standards and Department policies that govern confidentiality of the protected health information (PHI) and other confidential information (together, "Protected Information" or "PI") of our consumers. Department workforce members will use or disclose PI only as required by our job descriptions or as permitted or required by law, and will limit the PI used or disclosed to the minimum necessary to accomplish the intended purpose of our work, consistent with our Minimum Necessary Policy. Violations of HIPAA/HITECH or other applicable federal or state confidentiality requirements will be investigated and may result in application of workplace sanctions, up to and including termination from employment, consistent with our Privacy and Security Sanctions Policy.

III. RATIONALE

The Department is required by a variety of legal mandates to protect the confidentiality of PI. For example, the HIPAA Privacy Rule addresses how HIPAA-covered entities, such as our healthcare providers and payer (MaineCare), may use and disclose PI, and grants certain privacy rights to individuals regarding their PI. The Security Rule specifies a series of administrative, physical, and technical safeguards, as well as organizational requirements, to ensure the confidentiality, integrity, and availability of our electronic PI (ePI). HITECH Breach Notification and Enforcement Rules underscore the importance of our vigilance in protecting PI. Other federal laws, as well as state laws, licensing rules and accreditation standards add additional requirements and layers of protection with which the Department must comply.

Both HIPAA and HITECH mandate numerous step-by-step compliance requirements, and failure to meet these requirements could subject the Department to investigation, notice to the media and individual consumers, substantial civil monetary (enforcement) penalties, and, in certain cases, criminal prosecution.
IV. PROCEDURES

A. **Responsibility** - The Director of Healthcare Privacy shall have overall responsibility for the administration of this policy. Privacy/Security Liaisons shall have responsibility for the administration of this policy in their respective program areas and facilities.

B. **Designation of Privacy/Security Liaisons** – Directors and/or Superintendents shall appoint Privacy/Security Liaisons for their Offices, Programs, and/or Facilities that create, receive or maintain PI.

C. **Duties of the Privacy/Security Liaison** - Privacy/Security Liaisons shall assist the Director of Healthcare Privacy and perform the following tasks, including:

   i. Implementing Department privacy and confidentiality policies, forms and practices in their respective offices and entities;
   
   ii. Reinforcing and/or providing, as determined by the Director of Healthcare Privacy, program/facility specific training and otherwise acting as an information resource for staff;
   
   iii. Receiving and addressing complaints regarding policy and compliance in collaboration with the Director of Healthcare Privacy;
   
   iv. Monitoring staff compliance, promptly reporting concerns, complaints, and actual or potential violations or security/privacy incidents to the Director of Healthcare Privacy, and assisting the Director of Healthcare Privacy in any privacy/security investigation pertaining to the Privacy/Security Liaison's area of authority;
   
   v. Maintain program/facility compliance records, and provide periodic written and verbal reports to the Director of Healthcare Privacy.

D. **Privacy/Security Liaison Meetings**: - The Director of Healthcare Privacy shall hold periodic meetings with Privacy/Security Liaisons to review concerns, policies, processes, requirements and reports, and to provide education and updates as necessary to meet HIPAA, HITECH, and other applicable federal and state law privacy and security compliance standards.

V. DISTRIBUTION

All Department employees via e-mail and posting on the DHHS intranet.

December 14, 2018
Date

Bethany Hamm
Acting Commissioner